>> are most likely to be interested in their product. Unfortunately, they do not always choose to keep the information they pharm private.

"A lot of the people who have this information didn't get it illegally," Finley said. They got it from people you do business with online. Nine out of 10 companies these days sell their client lists to other people.

"They need money and sell their lists," he continued. "The problem is they don't always sell them to other legitimate companies."

Personal information can also be pharmed from hackers who redirect you from a legitimate website to an imposter site to harvest personal data. Social networking sites like Facebook and Twitter are increasingly being targeted in these scams.

Social networking sites are also places where people need to be careful about how much information they put out there. Information such as full birth date, geo tags on uploaded photos, maiden names, high school, family members and sometimes even addresses and phone numbers, easily found on social networking sites, give thieves ample information to steal an identity. People aren't thinking through what information they allow to be put out to their supposed "friends," DOCJT's McKinney said.

"We have a lot of kid victims — for a generation that is so technically savvy, they are so technically stupid," Finley said about the ways young people share information online. "Sometimes the technology goes far beyond the ability of people to use common sense. The more information you make available, the more likely you are to be a victim of identity theft in any of its forms. You have to be smart about it. … Maintain control of your information.

> *The more information you make available, the more likely you are to be a victim of identity theft in any of its forms.*

"Facebook changes stuff all the time and their policy is you have to opt out, not opt in," Finley continued. "[You] have to check the settings almost daily to keep things hidden. For every one button you click, there's three back doors to get into that same thing. So, you have to check them all, all the time. Anything you put out there — well, if it's out there, it's out there forever."

I SPY … SOMETHING STOLEN

Spyware is illicit software that can unknowingly be downloaded when an email attachment is opened, a pop-up window is clicked or a corrupted song or game is downloaded. Sometimes the phishing emails sent out are harmless in and of themselves, Finley said. They don't ask the person to verify information, but when clicked on, a piece of spyware or malware downloads to the computer that logs key strokes and allows the thief to watch every move the user makes.

"Now they have all your passwords and log ins and they can get to all your accounts," Finley said. "They have full access to everything on your computer at that point. Some can even search your files."

Finley recommends purchasing good, reliable anti-virus software in order to prevent spyware identity theft. Having good software and being sure to keep it current can protect individuals from most of these types of unknown information theft on the computer. Software such as the Norton Security suite or Kaspersky cost approximately $70 and can be placed on several computers, and cost an additional $20 a year to keep current, Finley said.

"That's the best money you can spend if you're going to be online," he said. "It can scan and take that [junk] off and can block anything coming in and anything going out."

GOT MAIL?

With all the sophisticated computer scams out there these days, it may be easy to forget the simplicity of good old-fashioned pick pocketing, mail theft and people rooting through trash looking for information worth taking. There are lots of little steps individuals can take every day to protect their personal financial and account information from traditional forms of identity theft.

"A cheap insurance policy is a shredder," Finley said. "Make sure you get one